9. Exercise sheet

If you find any errors in the sheets, do not hesitate to write an email to the mailing list 11ws-ac@lists.bit.uni-bonn.de.

Exercise 9.1 (SHA-3 candidates). (10 points)
On the website http://csrc.nist.gov/groups/ST/hash/sha-3/Round3 submissions_rnd3.html you find the five SHA-3 finalists. Give a justified recommendation which one you find best suitable for lightweight applications. Furthermore compare your selection to the PRESENT-based constructions of hash functions in terms of speed, space-requirements and security.

Exercise 9.2. (15+5 points)
Implement DM-PRESENT-80. Find a collision.

Why is your collision not a security threat in lightweight scenarios?